each and every element claimed by Applicants is found in the Kennedy, et al. reference. The Examiner in his rejections in the above-noted Office Action cites the specific language found in Applicants' claims and bases his anticipation rejections on excerpts which, in fact, do not support his assertions and are taken out of context.

The Examiner's rejections are quoted *verbatim* and listed *seriatem*, with Applicants' responses to the specific rejection presented immediately thereafter.

The Examiner says: "As to claim 1, Kennedy et al. discloses a method for setting basic means of access for operation of devices of which the operation is controllable by electronic means, comprising: the devices comprising mobile phones, small computer-controlled consumer devices with relatively low level of computing power, computers, motor vehicles, control terminals for industrial processes, all of which devices may require authentication prior to operation [Column 3, lines 47-62]..."

Response: Applicants respectfully submit that Kennedy et al. do not disclose the variety of devices that are claimed by Applicants. In Column 3, lines 47-62, which is the supporting basis of the rejection, Kennedy is only referring to cellular phones or personal communication devices. There is no mention of the other devices. There is no basis upon which to expand the teaching.

The present invention can be used by a particular software application on the system to verify access authorization. This could be a single software application, which evaluates the security token and is running on top of the used hardware. Applicants detail the usage of the token to provide specific configuration information, which defines constraints for the usage of a particular user. This "constraint" e.g. temporary deactivation, limits the usage of a reduced feature set. This is more than just "authentication". It adds "authorization" patterns. The support for this is disclosure is found at page 15, the last full paragraph: "A company telephone system consists of 20 telephones hierarchically grouped into three levels, with corresponding scopes of functions. The telephone

sets themselves are produced uniformly and are assigned their
actual features only by means of the configuration procedure,
which enables or disables various logic components in the sets
depending on the customer's specific requirements."

To reiterate, Applicants are entitled to retain mobile phones as one of the functioning devices in
their invention in view of the limitations now found in Claim 1. An important feature of the
present invention, is access to different (software) functions, based on the privileges of the user
who identified himself/herself to the system.

"establishment of a link between a personal authentication
system supplied with encryption data and a logic system able to
control an electronic device control, the encryption being
stored solely in the authentication system, the link between the
authentication system and the device being via wired of wireless
means [Column 4, line 57 to Column 5, line 15]."

Response: Applicants are not sure of the relevance of the cited excerpt with respect to the instant
invention. At the cited text, Kennedy, et al. are setting up a connection between the smart card
and the cellular phone, but they are using a completely different security system to do so. It is
essential to note in properly evaluating the overall system disclosed by Kennedy, et al. that a
part of an algorithm has to be stored on the smart card (Column 3, line 10 - 21), the other part on
the device in question. Applicants' Claim 1 distinguishes their invention from Kennedy by
reciting that: "*said encryption data being stored solely in said authentication system.*" In the
event a public or private key infrastructure is used, the required keys are stored in their entirety;
for example, on the smart card as well as on the device. In Applicants' invention, a key may be
present on the device and the same key on the smart card, so a challenge/response can be used to
authenticate the smart card. However Applicants are not splitting the key (as Kennedy, et al.)
such that the first 64 bits of the key are on the card and the remaining 64 bits (in the case of a
128 bit key) are on the device. Applicants now positively recite that they use a "*non-split key*"

The Examiner continues with his rejection referring to the next portion of Claim 1:

```
"checking the encryption data in the authentication system prior
to operation of the electronic device control [column 5 line 30
to column 6 line 5];"
```

It appears in Kennedy that the user is granted access to the contents of the personal computer as well as its networked resources. This means that there is only one level of authentication (access yes/no). The present invention solves the need to have different levels of access where in claim 1, Applicants claim: *"...enabling of the means of access predetermined for the authentication system dependent on the result of the check."*

Please note that in Kennedy, Column 5, lines 50-51, the credentials are loaded from the card on the host. In Applicants' invention, there is no need to transfer the credentials to the host. In particular it is preferable to keep the credentials on the smart card.

```
"assignment of predetermined means of access to the electronic
device control associated with the authentication system the
predetermined means providing access to the physical hardware
resources and access to different software functions, based on
the privileges of the user who identified himself to the system,
the software function evaluates a security token and is running
on top of the physical hardware [Column 4, lines 39-56"
```

Response: In the Kennedy, at al. patent, when considering *"access,"* there is only one level of access. An important distinguishing key to the present invention is that there are different levels of access to differentiate the different levels of authentication or authorization that persons with different roles may need. The Examiner is referred to page 6 of the instant specification. The different levels are mentioned on page 6. At that location, there is a disclosure of the system being open to progressive hierarchies of access rights to the device, for example, by the production of a Master SmartCard which can be issued to customers' service personnel in order to configure large numbers of individual devices.

Further, on page 6: "Applying the method in accordance with the invention, and based on the stipulation that a single SmartCard is to be able to configure any number of devices but that only a Master SmartCard or a personal SmartCard can be used to shut down and/or startup/restart the devices, a device manufacturer may do the following..."

Applicants differentiate between a single (standard) smart card and a Master Smart Card. The different levels are mentioned in the portion of Claim 1 that reads: "...assignment of <u>a plurality of</u> predetermined means of access to the device associated with the authentication system." Applicants' Claim 1states:

"said predetermined means of access being dependent upon the level of authorization that is set in said personal authorization system."

"enabling of the means for access predetermined for the
authentication system dependent on the result of the check.
[Column 5, line 30 to column 6, line 5]"

Response: Applicants cannot locate any teaching or disclosure related to a multi-level security system in Column 5, line 30 to Column 6 line 5, quoted by the Examiner. Kennedy, et al. only refers to one level of security. The reference only refers to the manner in which the authentication is performed by using "split keys." There is no differentiation based on the role of the user. Applicants do not teach the use of the "split keys" in their invention. Claim 1 now reads, in pertinent part: *"... establishment of a <u>non split-key</u> link between a personal authentication system supplied with encryption data and a logic system able to control an electronic device control, said encryption data being stored solely in said authentication system..."*

the method providing means of no access or full access and allow
more finely defined levels of access as defined in a user
profile for configuration or maintenance work [column 4, lines
39-56].

Response: Applicants cannot locate any teaching or disclosure related to "no access or full access and allow more finely defined levels of access" as defined in a user profile for configuration or maintenance work at the location in Kennedy cited by the Examiner. In light of Kennedy's teaching as delineated in the claims of the patent, it is clear that Kennedy is talking about different levels of secure communication, and the means of access to the aforementioned different levels of secure communication. Note that the access in Kennedy is achieved (controlled) by different access algorithms (Column 4, line 42), and not by a different key as is taught by Applicants.

The Examiner continues: "As to claim 2, Kennedy et al. disclose that the basic means of access of functions of the device comprise at least one of the following means: disable operation of the devices, enable operation of the devices, or enable configuration of device. [Column 5, line 30 to column 6, line 5]."

Response: There is no mention of enabling the configuration of the device in Kennedy, et al. Column 5, line 30 to column 6, line 5. A careful reading of the section reveals that it only refers to access or not. Thus, there is no anticipation of the elements defined in Claim 2.

The Examiner continues: "as to claim 3, Kennedy at al. disclose that the link is made without need for intermediate software layers. [Column 3, lines 63-67]."

Response: There is no mention that the link is made without the need for an intermediate software layer in Kennedy, et al. at Column 3, lines 63 – 67. Column 3, lines 63 – 67 only discusses the "token" and NOT how the link is set up. Further the excerpt teaches that it basically is comprised entirely of software. Applicants' system uses no software so there is no anticipation of the elements defined in Claim 3.

The Examiner continues: "As to claim 4, Kennedy et al. disclose in addition, the step of reading at least one of the following features embodied within the authentication system: firmware programs, device-specific command sequences for execution of specific device-specific functions, cryptographic keys, cryptographic algorithms, and individual decision-making logic. [Column 4, lines 39-56]."

Response: There is <u>no</u> mention of the step of reading at least one of the features embodied within the authentication system in Kennedy, et al. at Column 4, lines 39-56. In this excerpt, Kennedy only refers to secure transmission or accessing the database that the host contains to store some decrypted data. He notes that there are keys and alogorithms stored in this data base. This would suggest it proper to infer that there are two data bases covered by Kennedy, but not others. Thus, again, there is no anticipation of the elements defined in Claim 4.

The Examiner continues: "As to claim 10, Kennedy et al. disclose program code areas for the execution or preparation for execution of the steps when the program is installed in a computer. [Column 3, lines 8 - 46]."

Response: Applicants can find no relevance in the disclosure at Column 3, lines 8 – 46 relating to the content of Claim 10 and request specific clarification as to the relevance of the cited lines in Kennedy, et al. to Claim 10. The excerpt refers to how the split key algorithm is used to get access. The Kennedy disclosure at the cited location has no teaching of installing a computer program on the host.

The Examiner continues: "As to claim 11, Kennedy et al. discloses a means for setting basic means of access for operation of devices of which the operation is controllable by electronic means, comprising: [the balance of the claim is as defined in claim 1].

Response: The responses to each of the elements as set forth above is incorporated by reference herein.

The Examiner is respectfully requested to reconsider his rejection of claims 5 - 9 under 35 U.S.C. §103(a) as being unpatentable over United States Patent 6,084,968 to Kennedy, et al. as applied to Claim 1, and further in view of United States Patent 6,415,144 to Findikli, et al.

The Examiner concedes that Kennedy does not teach that the method disclosed therein includes (1) configuration of the devices by authorized persons, and (2) that after successful authentication device specific configuration data are downloaded into the devices from the authentication system in accordance with the authentication system or over a network. With respect to the latter missing element, Applicants reiterate that Kennedy do not disclose the variety of devices that are claimed by Applicants. In Column 3, lines 47-62, which is the supporting basis of a rejection noted above, the reference is only referring to cellular phones or personal communication devices. There is no mention of the other devices. There is no basis upon which to expand the teaching. It is improper to expand the scope of the disclosure to devices other than cellular phones and the like when no positive recitation is found in the art which supports the assertion.

Kennedy relates to a split key system. The Kennedy invention is specifically tailored to operate in a certain manner and is characterized as an improvement over the prior art in which the problems therewith are discussed in Column 2, lines 35 – 46. His improvement is a host apparatus which has multiple secure functions which are accessed by a token or smart card.

Findikli discloses a method of message management using a mobile communications device with a core and protected memories. Findikli, at Column 1, line 61 to Column 2, line 5 provides a general description of two over-the-air teleservices with no specific direction of how either of the systems listed is used in conjunction with a specific system. The excerpt cited by the Examiner as being relevant is merely a description of the prior art as known when the application was filed. As to tailoring the cellphones to meet the needs of the subscriber, Findikli states that the systems mentioned would not be effective if the phones had been hard-coded to prevent overwrite. The

skilled artisan would not combine the two references as each is so specific as to be unique in its manner of operation leaving no room for combining with the other. The Examiner cites Findikli saying over-the-air teleservices provide radio telecommunications operators with greater flexibility in tailoring wireless devices to meet the needs of their subscribers. The real task is in the detail of explicating how the "tailoring" is done. There is no basis to extrapolate the cited excerpt to assert that is says any more than what it specifically does disclose.

The Examiner acknowledges that Kennedy, et al. does not teach the method including configuration of the devices by authorized persons. With regard to claim 5, Findikli, et al. teach download of configuration information, in an unsecure way. There is no connection to any security system on the device. There is also no way to personalize/customize the configuration without the mobile phone being registered with a service provider, which may not always be the case for all the devices (like to a landline phone, or a washing machine). There is no basis to combine these references.

As to the rejection of Claim 6, Kennedy only refers to secure transmission or accessing the database that the host contains to store some decrypted data. He notes that there are keys and alogorithms stored in this data base. This would suggest it proper to infer that there are two data bases covered by Kennedy, but not others. No proper basis to combine the two references.

As to the rejection of Claim 7, Kennedy doesn't teach the access of different groups or people with different roles.

As to Claims 8 and 9, there is no basis for combining the references. It was demonstrated above that Kennedy and Findikli do not describe the inventions that warrant the proposed combination. These references, alone or in combination do not disclose the invention defined in claims 8 and 9.

Kennedy, et al. and Findikli, et al., alone, or in combination, do not disclose or even imply the elements of Claims 5 - 9 of the present invention. In the rejection, the Examiner is selectively picking and choosing individual elements disclosed in the references to the exclusion of what the references as a whole teach to one skilled in the art.

In order to analyze the propriety of the Examiner's rejections in this case, a review of the pertinent applicable law relating to 35 U.S.C. § 103 is warranted. The Examiner has applied the Kennedy, et al. and Findikli, et al. references discussed above using selective combinations to render obvious the invention.

The Court of Appeals for the Federal Circuit has set guidelines governing such application of references. These guidelines are, as stated are found in Interconnect Planning Corp. v. Feil, 774 F.2d 1132, 1143, 227 USPQ, 543, 551:

> **When prior art references require selective combination by the court to render obvious a subsequent invention, there must be some reason for the combination other than hindsight gleaned from the invention itself.**

A representative case relying upon this rule of law is Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 5 USPQ 2d 1434 (Fed. Cir. 1988). The district court in Uniroyal found that a combination of various features from a plurality of prior art references suggested the claimed invention of the patent in suit. The Federal Circuit in its decision found that the district court did not show, however, that there was any teaching or suggestion in any of the references, or in the prior art as a whole, that would lead one with ordinary skill in the art to make the combination. The Federal Circuit opined:

> **Something in the prior art as a whole must suggest the desirability, and thus the obviousness, of making the combination.** [837 F.2d at 1051, 5 USPQ 2d at 1438, citing Lindemann, 730 F.2d 1452, 221 USPQ 481, 488 (Fed. Cir. 1984).]

The Examiner in his application of the cited references is improperly picking and choosing. The rejection is a piecemeal construction of the invention. Such piecemeal reconstruction of the prior

art patents in light of the instant disclosure is contrary to the requirements of 35 U.S.C. § 103.

> **The ever present question in cases within the ambit of 35 U.S.C. § 103 is whether the subject matter as a whole would have been obvious to one of ordinary skill in the art following the <u>teachings</u> of the prior art at the time the Invention was made. It is impermissible within the framework of Section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art. (Emphasis in original)** <u>In re Wesslau</u> 147 U.S.P.Q. 391, 393 (CCPA 1965)

This holding succinctly summarizes the Examiner's application of references in this case, because the Examiner did in fact pick and choose so much of the Findikli, et al. reference with respect to "device specific configuration data" to support the rejection and did not cover completely or accurately in the Office Action the full scope of what these varied disclosure references fairly suggest to one skilled in the art.

Further, the Federal Circuit has stated that the Patent Office bears the burden of establishing obviousness. It held this burden can only be satisfied by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the reference.
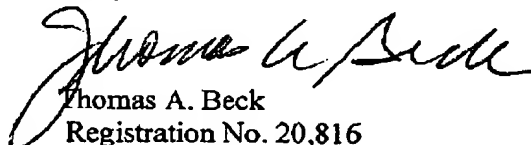
> **Obviousness is tested by "what the combined teachings of the references would have suggested to those of ordinary skill in the art."** <u>In re Keller,</u> 642 F.2d 413, 425, 208 USPQ 871, 881 (CCPA 1981). **But it "cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination."** <u>ACS Hosp. Sys.,</u> 732 F.2d at 1577, 221 USPQ at 933. [837 F.2d at 1075, 5 USPQ 2d at 1599.]

The Court concluded its discussion of this issue by stating that teachings or references can be combined <u>only</u> if there is some suggestion or incentive to do so.

In the present case, the skilled artisan, viewing the references would not be directed toward Applicants' system. There can reasonably be no system such as Applicants emanating from the Kennedy, et al. and Findikli, et al. references as the basic focus of the two references are different. There is no proper basis to combine them.
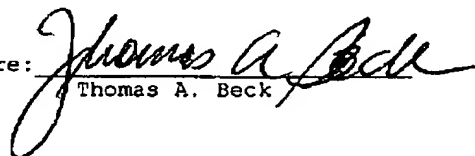
Applicants have attempted in this response to include language limitations to specifically define the invention and to clear up any ambiguities that may have existed in the wording heretofore. Applicants believe that the amended claims are in a form which should result in their allowability. If there are additions which could result in the claims being allowed, Applicants' attorney would be pleased to speak with the Examiner by phone concerning such action at a mutually agreeable time and will cooperate in any way possible.

Respectfully Submitted,

Thomas A. Beck
Registration No. 20,816
26 Rock Ledge Lane
New Milford, CT 06776
(860) 354-0892

I hereby certify that this amendment response is being telefaxed to Examiner Moorthy at (571) 273-8300 on the date indicated below addressed to Commissioner of Patents & Trademarks, Post Office Box 1450, Alexandria, VA 22313-1450

Signature: _____   Date: August 16, 2006
Name: Thomas A. Beck